

In re Patent Application of:
SONZOGNI ET AL.
Serial No. **Not Yet Assigned**
Filed: **Herewith**

a microprocessor including an operating system working with a set of instructions, said microprocessor comprising a first register for storing a first code, on at least one check bit, for an entity to be executed, said first register being updated based upon a call instruction and a return instruction during execution of a new entity;

a memory connected to said microprocessor for storing a plurality of application programs; and

a checking device connected to said microprocessor for checking, as a function of the at least one check bit, whether access to locations in said memory is authorized for the new entity.

6. A chip card according to Claim 5, wherein said microprocessor comprises a second register for storing a second code for the application programs active when a last call instruction was sent.

7. A chip card according to Claim 6, wherein said second register can not be directly accessed.

8. A chip card according to Claim 5, wherein each entity is one of the plurality of application programs.

9. A chip card according to Claim 5, wherein each entity causes a hardware event.

10. A chip card according to Claim 9, wherein the hardware event resets said microprocessor.

In re Patent Application of:
SONZOGNI ET AL.
Serial No. **Not Yet Assigned**
Filed: **Herewith**

11. A chip card according to Claim 5, wherein said first register is updated in response to the return instruction.

12. A chip card according to Claim 5, wherein said checking device provides a control signal to said microprocessor for providing access to the locations of said memory if the new entity is authorized.

13. A chip card according to Claim 5, wherein said checking device compares the address locations to be accessed in said memory and the first code in said first register.

14. A chip card comprising:
a microprocessor comprising

a first register for storing a first code, on at least one check bit, for an application program to be executed, said first register being updated based upon a call instruction and a return instruction during execution of a new application program, and

a second register for storing a second code for an application program active when a last call instruction was sent;

a memory connected to said microprocessor for storing the application program; and

a checking device connected to said microprocessor for checking, as a function of the at least one check bit, whether access to locations in said memory is authorized for the new application program, said checking device providing a control signal to said microprocessor for providing access to

In re Patent Application of:
SONZOGNI ET AL.
Serial No. **Not Yet Assigned**
Filed: **Herewith**

the locations of said memory if the new application program is authorized.

15. A chip card according to Claim 14, wherein said second register can not be directly accessed.

16. A chip card according to Claim 14, wherein each application program causes a hardware event.

17. A chip card according to Claim 16, wherein the hardware event causes said microprocessor.

18. A chip card according to Claim 14, wherein said first register is automatically updated in response to the return instruction.

19. A chip card according to Claim 14, wherein said checking device compares the address locations to be accessed in said memory and the first code in said first register.

20. A method for securing access to a chip card comprising a microprocessor including an operating system working with a set of instructions, and a memory connected to the microprocessor for storing a plurality of application programs, the method comprising:

storing a first code, on at least one check bit, in a first register of the microprocessor for an entity to be executed;

updating the first register based upon a call instruction and a return instruction during execution of a new entity; and

In re Patent Application of:
SONZOGNI ET AL.
Serial No. **Not Yet Assigned**
Filed: **Herewith**

checking, as a function of the at least one check bit, whether access to locations in the memory is authorized for the new entity.

21. A method according to Claim 20, further comprising storing a second code in a second register of the microprocessor for an application program active when a last call instruction was sent.

22. A method according to Claim 21, wherein the second register can not be directly accessed.

23. A method according to Claim 20, wherein each entity is one of the plurality of application programs.

24. A method according to Claim 20, wherein each entity causes a hardware event.

25. A method according to Claim 24, wherein the hardware event resets the microprocessor.

26. A method according to Claim 20, wherein the first register is updated in response to the return instruction.

27. A method according to Claim 20, wherein checking comprises providing a control signal to the microprocessor for providing access to the locations of the memory if the new entity is authorized.

090114100040
A1
CONF

In re Patent Application of:
SONZOGNI ET AL.
Serial No. **Not Yet Assigned**
Filed: **Herewith**

28. A method according to Claim 20, wherein checking comprises comparing the address locations to be accessed in the memory and the first code in the first register.

29. A method for securing access to a chip card comprising a microprocessor and a memory connected thereto for storing a plurality of application programs, the method comprising:

storing a first code, on at least one check bit, in a first register of the microprocessor for an application program to be executed;

updating the first register based upon a call instruction and a return instruction during execution of a new application program; and

checking, as a function of the at least one check bit, whether access to locations in the memory is authorized for the new application program.

30. A method according to Claim 29, further comprising storing a second code in a second register of the microprocessor for an application program active when a last call instruction was sent.

31. A method according to Claim 29, wherein the second register can not be directly accessed.

32. A method according to Claim 29, wherein each application program causes a hardware event.

CONFIDENTIAL
COPY